WARD, KEENAN & BARRETT, P.C.
Gerald Barrett, SBN: 005855
3838 N. Central Avenue, Suite 1720
Phoenix, Arizona 85012
Tel: (602) 279-1717
Fax: (602) 279-8908
E-Mail: gbarrett@wardkeenanbarrett.com

BURSOR & FISHER, P.A.
Neal J. Deckant (*Pro Hac Vice*)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ndeckant@bursor.com

BURSOR & FISHER, P.A.
Joshua D. Arisohn (*Pro Hac Vice*)
Alec M. Leslie (*Pro Hac Vice*)
Max S. Roberts (*Pro Hac Vice*)
888 Seventh Avenue
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jarisohn@bursor.com
aleslie@bursor.com
mroberts@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Carol Davis, individually and on behalf of all others similarly situated,

Plaintiff,

v.

HDR, Inc.,

Defendant.

Case No. 2:21-CV-01903-SPL

FIRST AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Carol Davis ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself and her counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought against Defendant HDR, Inc. ("HDR" or "Defendant") for collecting the electronic communications of members of the following private Facebook groups (the "Group Members"): Ahwatukee411 and Protecting Arizona's Resources & Children (PARC) ("PARC") (collectively, the "Private Facebook Groups") without authorization or consent. Defendant uses a sophisticated "social listening" service to secretly observe and monitor Group Members' electronic communications and confidential postings in the Private Facebook Groups, through the use of monitoring tools, automated software, and dedicated employees with backgrounds in signals intelligence and communications intelligence. As such, Defendant has violated the Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq.*, violated the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*, and violated the Group Members' common law right to privacy.

2. Plaintiff Davis is a member of the Private Facebook Groups, Ahwatukee411 and PARC. Plaintiff Davis communicated with other Group Members in the Private Facebook Groups, and her communications were monitored, captured, and analyzed by Defendant.

3. Defendant HDR is a multi-billion-dollar architecture and design firm that has designed over 275 jails and prisons, and also offers various covert surveillance services. Defendant monitored the Private Facebook Groups secretly and without consent, and gathered information about discussions in the groups in order to inform Defendant's and its client's marketing strategies.

4. Defendant conducted this monitoring by hiring employees and

investigators with backgrounds in intelligence, particularly geospatial and information management, and strategic communications. These employees, operating as part of Defendant's "STRATA" team, deployed automated tools and monitoring software and otherwise infiltrated the Private Facebook Groups on behalf of HDR.

5. Plaintiff brings this action on behalf of herself and a class of all persons whose electronic communications in the Private Facebook groups were secretly monitored and by Defendant's wiretaps.

THE PARTIES

6. Plaintiff Carol Davis is a citizen of Arizona who resides in Phoenix, Arizona with an intent to remain there. Plaintiff Davis has been a member of the Private Facebook Group, Ahwatukee411, since approximately 2015. Since 2015, and prior to the filing of this lawsuit, Plaintiff Davis posted in the Ahwatukee411 Private Facebook Group and communicated with other Group Members. Plaintiff Davis's posts discuss topics such as recommendations for services and debates involving local issues, such as the construction of a local highway and potential political corruption. Plaintiff Davis regularly posts in the Ahwatukee411 Facebook group approximately two to three times a week, and her most recent post was in October 2021. Plaintiff Davis was in Phoenix, Arizona when she accessed and posted in the Ahwatukee411 Private Facebook Group. Since at least 2016, if not earlier, Plaintiff Davis's private electronic communications with other Group Members, including her communications regarding recommendations for services and debates involving local issues, were monitored, read, disclosed, intercepted in real-time, and otherwise wiretapped and/or accessed in electronic storage by HDR. Plaintiff Davis was unaware at the time that her electronic communications, including the information described above, were being intercepted in real-time and would be disclosed to HDR, nor did Plaintiff Davis consent to the same.

7. Plaintiff Davis has also been a member of the Private Facebook Group,

PARC, since approximately 2016. Since 2016, and prior to the filing of this lawsuit, Plaintiff Davis posted in the PARC Private Facebook Group and communicated with other Group Members. Plaintiff Davis's posts discussed topics such as debates over the construction of a local highway and its environmental impact. Plaintiff Davis often posts in the PARC Facebook group, and her most recent post was in approximately August 2021. Plaintiff Davis was in Phoenix, Arizona when she accessed and posted in the PARC Private Facebook Group. Since at least 2016, if not earlier, Plaintiff Davis's private electronic communications with other Group Members, including her communications regarding debates involving local issues, were monitored, read, disclosed, intercepted in real time, and otherwise wiretapped and/or accessed in electronic storage by HDR. Plaintiff Davis was unaware at the time that her electronic communications, including the information described above, were being intercepted in real-time and would be disclosed to HDR, nor did Plaintiff Davis consent to the same.

8. Defendant HDR, Inc. is a Delaware Corporation with its principal place of business at 1917 S. 67th Street, Omaha, Nebraska 68106.

9. HDR does business throughout Arizona and the entire United States. HDR contracts with numerous clients, including the Arizona-based clients that authorized the conduct here.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, and at least one member of the proposed class is a citizen of a state different from Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant has purposefully availed itself of the laws and benefits of doing business in this State, and Plaintiff's claims arise out of Defendant's forum-related activities. Furthermore,

a substantial portion of the events giving rise to Plaintiff's claims occurred in this District.

12. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

STATEMENT OF FACTS

I. Overview Of The Wiretaps

A. Defendant's STRATA Social Medial Listening Service

13. HDR is a multi-billion-dollar architecture and design firm that has designed over 275 jails and prisons.

14. In addition to its architectural services, HDR also offers a number of other services to its clients. One of HDR's services is its "Strategic Communications" team, which "works to help our clients manage the social and political risk associated with infrastructure development …. Our teams leverage web, video and social networking and are experienced with wide-scale media campaigns that include targeted digital, print, television and radio material."

15. Another service offered by HDR is its Geospatial and Information Management team, which "secur[es], organiz[es] and present[s] digital information for easier access and informed decision-making. We collaborate with clients to automate workflows, connect systems, create reports and, ultimately, increase productivity."

16. HDR's "Strategic Communications" and "Geospatial and Information Management" teams "jointly execute" another service offered by HDR, its "STRATA" service.

17. STRATA is a surveillance or "social listening" service that "uses data to inform and enhance [HDR's] approach to public understanding. Our STRATA team practices data-driven engagement beyond standard demographics, and tailors public involvement and decision-making approaches specifically for every project."

18. As HDR formerly advertised on its website,[1] the goal of the STRATA service "is to gauge and mitigate social and political risks before they affect a project …. To be candid, STRATA exposes the truth of the human experience through comprehensive analysis from a technical and empathic lens."

19. In order to achieve these objectives, the STRATA service:

> [L]everage[s] commercial off-the-shelf tools to develop powerful applications for communication strategies and issues mapping. **These tools enable us to extract, analyze and present demographics, lifestyle patterns and behaviors, and market potential indices to better understand the overall community.** We can quickly generate reports, interactive maps, dashboards and infographics to create powerful visual profiles and to assess potential social and political risks.

20. The effect of this monitoring, Defendant claims, is saving its clients money: "Controversy is costly, both in reputation and in dollars. Social and political risk deserves attention at the planning stage of a project or program, where it can be carefully assessed and when there is time to develop strategies to mitigate or diminish risk." Such activity is known as "corporate counterinsurgency."

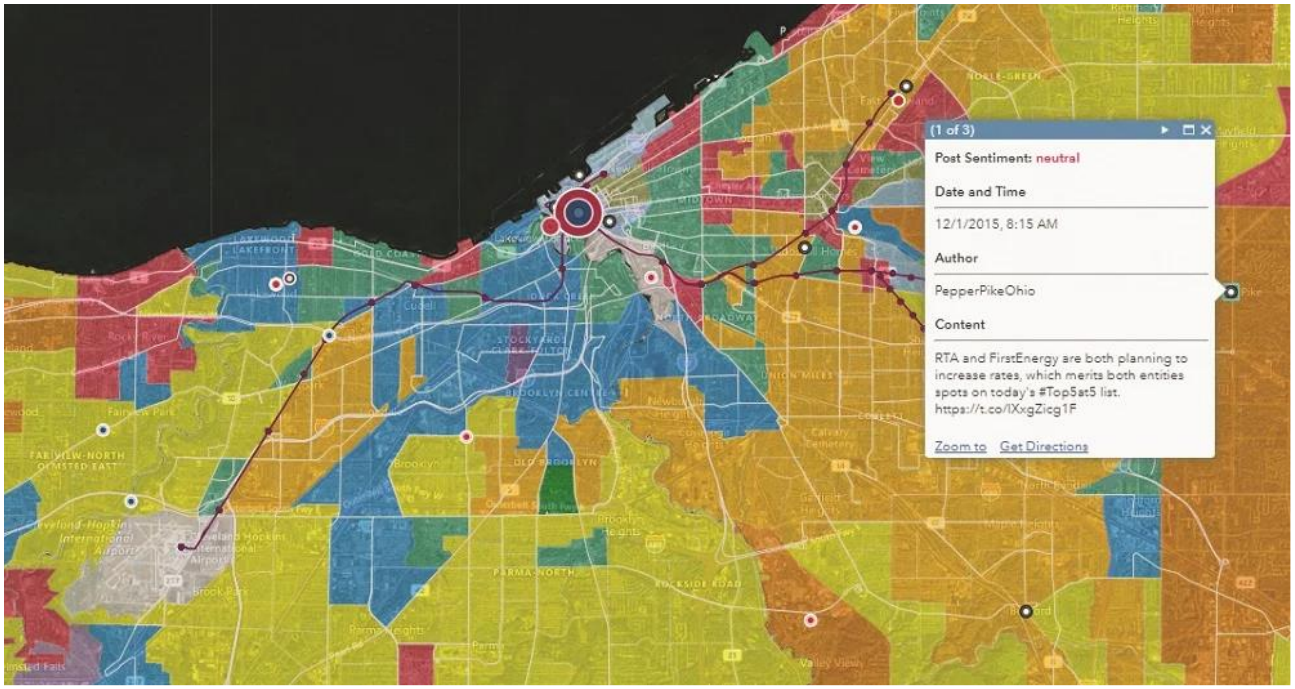
21. According to John Stauber, an author and expert on industry manipulation, the purpose of HDR's surveillance is to "survey[] and evaluat[e] public opinion, the leadership of potential opposition groups, and citizen activists who seek to change, delay or halt a multi-million dollar project."

22. Defendant states that the STRATA team can deliver "insights" in various forms: "Deliverables range from Excel reports to comprehensive web-based maps. Example datasets include project data, community profiles, poverty/income, education, employment, business summaries, race, language, digital usage and at-risk communities."

---

[1] HDR removed references to its STRATA service from its website in or about August 2021, after reporting by the publication *Vice* exposed HDR's illegal wiretapping.

23. Below is an example of a "comprehensive web-based map" that the STRATA team can generate. The map shows the location of a poster on a social media website, the content of a post, the post's author, the date and time of a post, and the "sentiment" of a post:



24. In short, Defendant claims that the "STRATA team can provide **24/7 listening on social media platforms** and use sentiment analysis to determine trends, specify key influencers and identify or mitigate risk. Social media listening allows us to track project success by measuring the effectiveness of messaging and communication. Through social media listening, we can answer the following questions throughout the life of any project:

- Who are we reaching?
- What are they saying?
- Where are they?
- What are we missing?"

B. An Overview Of Private Facebook Groups

25. Facebook allows users to create and join two different types of groups: public and private groups. As relevant here, in private Facebook groups, "only

members can see who's in the group and what they post."[2]

26. Once a private Facebook group is created, the group administrators *cannot* "change [the group] to public." The reason for this is to "protect the privacy of group members." The only change that can be made is that the administrator of a private Facebook group can allow the group to be searchable (visible) or not (hidden). Thus, once a private Facebook group is created, the posts of users and the content of the group remain private *forever*.[3]

27. Private Facebook group members also have access to the names of all users in the private Facebook group. Group members can also see when the number of members in a group increases. Thus, a member of a private Facebook group could investigate the names of group members and determine whether he or she feels comfortable continuing to post in the private Facebook group in light of the current membership.

28. Facebook also employs additional protections to further protect the privacy of its members. Namely, Facebook's Terms of Service state that users "may not access or collect data from our Products using automated means (without our prior permission) or attempt to access data you do not have permission to access."

29. Facebook also discusses data scraping in its frequently asked questions. Facebook notes that "[u]nauthorized scraping is often done in a way that disguises the activity so that it blends in with ordinary usage."

30. Further, in 2019, the Federal Trade Commission entered into a $5 billion settlement with Facebook that required Facebook to "submit to new restrictions and a modified corporate structure that will hold the company accountable for the decisions it makes about its users' privacy." As part of this settlement, the FTC required Facebook to implement certain protections to "Nonpublic User Information." The

[2] https://www.facebook.com/help/286027304749263?helpref=faq_content.

[3] https://www.facebook.com/help/286027304749263?helpref=faq_content.

FTC defined "Nonpublic User Information" as "any User profile information (i.e., information that a User adds to or is listed on a User's Facebook profile), or User-generated content (e.g., status updates, photos), ***that is restricted by one or more Privacy Setting(s)***."

C. Defendant Infiltrates The Private Facebook Groups

1. Background On The Private Facebook Groups

31. In approximately December 2014, the Ahwatukee411 Private Facebook Group was formed. Ahwatukee411 is a closed Facebook group that enables local residents of the Ahwatukee Foothills area to privately discuss issues concerning the community. The Ahwatukee411 group has approximately 32,400 members.

32. The Ahwatukee411 Private Facebook Group has always been a private Facebook group, and will thus remain a private Facebook group in perpetuity. In order to join the group, prospective group members are required to fill out a questionnaire discussing their involvement in the Ahwatukee community and their interest in joining the group as it relates to the community. This process is intended to ensure that only residents (*i.e.*, those with a vested interest in the Ahwatukee community) can join the group and are able to see other posts.

33. In approximately 2016, the Protecting Arizona's Resources & Children (PARC) Private Facebook Group was formed (although the PARC organization itself has been around since 1995). The PARC Private Facebook Group was formed to protest the construction of a highway that cuts through the Moahdak Do'ag Mountain (South Mountain), which is sacred to the local Native American community in Phoenix. The PARC Private Facebook Group enables its members to privately discuss local issues. The PARC group has roughly 930 members.

34. The PARC Private Facebook Group has always been a private Facebook group, and will thus remain a private Facebook group in perpetuity. In order to join the group, prospective group members are required to undergo a screening process. This process is intended to ensure that largely only residents (*i.e.*, those whose homes

would be affected by the construction of the local highway) can join the group and are able to see other posts.

35. The idea of the Private Facebook Groups is that they are private and only populated with Ahwatukee local PARC members, not other persons, and certainly not employees or personnel of Defendant. Indeed, the PARC Private Facebook Group is run by persons who oppose Defendant's interests/projects and the interests/projects of Defendant's clients.

36. In order to join both Private Facebook Groups, prospective group members have to undergo a screening process that discusses their interest in joining the groups. This is more sophisticated than simply clicking a button to state they are interested in joining. Instead, passing the screening process would require prospective group members to, among other things:

(a) Know of the existence of the Ahwatukee community and the issues surrounding the community, such as the construction of the highway, to even know to search for the Private Facebook Groups;

(b) Research the Ahwatukee community and the issues surrounding the community, such as by reviewing news articles concerning the construction of the highway or other social issues;

(c) Have substantial knowledge of the aforementioned issues; and

(d) Draft answers to the screening questions discussing the prospective member's interest in the community based on the aforementioned research, as well as stating where the prospective group member resides.

37. While the aforementioned information is technically "public knowledge," the time, effort, and knowledge one would have to accrue or devote to research to pass the screening process to join a Facebook group concerning a random community in Arizona is not something a member of the "general public" would ever

do in practice. Instead, such a screening process could only be passed by either (i) someone who is truthfully a member of the Ahwatukee community or is truthfully affected by the construction of the highway that was the subject of the PARC Private Facebook Group; or (ii) is a sophisticated social media listening company that specializes in exactly this type of research. Defendant is the latter.

2. Defendant's Unauthorized Surveillance Of The Private Facebook Groups

38. Unbeknownst to the Group Members, however, since at least 2016—and going back months if not years earlier—HDR has privately and without consent infiltrated, monitored, wiretapped, and/or accessed posts in the Private Facebook Groups.[4]

39. The posts in the Private Facebook Groups were "Nonpublic User Information" per the FTC settlement with Facebook because the posts were "user generated content" (*i.e.*, posts created by users on the Private Facebook Groups) that were restricted by "one or more privacy settings."

40. It is unknown how Defendant infiltrated these Private Facebook Groups—whether through the use of fake social media profiles or some other method. Defendant, in its Motion to Dismiss, did not discuss how it joined the Private Facebook Groups or present what answers it gave to the screening questions. Further, what is known is that neither Defendant nor its employees should have had access to the Private Facebook Groups, nor did the Group Members know Defendant had infiltrated the Private Facebook Groups nor consent to Defendant wiretapping their conversations.

41. Thus, the clear inference is that Defendant used deceitful and untruthful answers to the screening process for the Private Facebook Groups in order to gain

[4] Ella Fassler, *A Company That Designs Jails is Spying On Activists Who Oppose Them*, VICE, Aug. 17, 2021, https://www.vice.com/en/article/93ym4z/a-company-that-designs-jails-is-spying-on-activists-who-oppose-them.

unauthorized access to the same.

42. Had Defendant provided truthful answers to the screening questions, Defendant would not have been admitted to the Private Facebook Groups. Or, even if Defendant was, group members would have asked for Defendant to be removed, or reported Defendant to Facebook for violation of Facebook's Terms and Conditions.

43. Once Defendant infiltrated the Private Facebook Groups, it "generated an 'influencer' report, an analysis of public sentiment on social media platforms, and a geospatial analysis that placed communities into categories such as 'ethnic enclaves,' 'barrios urbanos,' 'scholars and patriots,' and 'American dreamers.'" The analysis also involving reading and analyzing the content of the posts in the Private Facebook Group for use in the "comprehensive web-based map" described above.

44. Defendant monitored and/or intercepted posts in the Private Facebook Groups in real time, and/or accessed the contents of the posts in the Private Facebook Groups in electronic storage.

45. Notably, Defendant's practices violated Facebook's Terms of Service, which state users "may not access or collect data from our Products using automated means (without our prior permission) or attempt to access data you do not have permission to access."

46. These processes, as currently employed by HDR, function as a wiretap, as well as the acquisition of electronic communications in electronic storage.

II. Defendant Collected Plaintiff's Electronic Communications

47. Since approximately 2015, Plaintiff has been a member of the Ahwatukee411 Private Facebook Group.

48. Plaintiff privately communicated with other Group Members in the Ahwatukee411 Private Facebook Group. Plaintiff communicated about topics such as recommendations for services and debates over local issues, including the construction of a local highway and potential political corruption.

49. Likewise, since approximately 2016, Plaintiff has been a member of the

PARC Private Facebook Group.

50. Plaintiff also privately communicated with other Group Members in the PARC Private Facebook Group. Plaintiff communicated about topics such as debates over the construction of a local highway and its environmental impact.

51. Plaintiff's posts in these Private Facebook Groups were "Nonpublic User Information" per the FTC settlement with Facebook, because the Private Facebook Groups are permanently private, and thus, Plaintiff's communications were restricted by "one or more privacy settings." Further, Plaintiff's communications were "user generated content."

52. To join both groups, Plaintiff went through a questionnaire and screening process to ensure she was an Ahwatukee resident and her interests were aligned with the PARC organization's goals.

53. In both the Ahwatukee411 and PARC Private Facebook Groups, Plaintiff believed she was only communicating with other Ahwatukee residents or members of the PARC organization. Plaintiff did not believe, nor did Plaintiff know or have reason to know, that her communications were being surveilled by unconsented-to third-party actors who were neither Ahwatukee residents nor persons whose interests were not aligned with the PARC organization's goals, and certainly not corporations antagonistic to the interests of the Private Facebook Groups.

54. Since at least 2016, Plaintiff's private posts—which are "Nonpublic User Information" per the FTC settlement—were tracked, read, intercepted, analyzed, and otherwise wiretapped and/or accessed in electronic storage by Defendant in real time using the aforementioned processes, and without Plaintiff's consent.

55. Plaintiff could have determined whether Defendant or its employees were group members by looking at the list of group members for each Private Facebook Group. Plaintiff would have seen if new members joined the Private Facebook Groups because she would have seen the number of group members

increased.

56. Had Defendant answered the screening questions truthfully, Plaintiff would have known Defendant had access to the Private Facebook Groups and chosen not to communicate with other group members, or would have informed the group administrators of Defendant's access to the Private Facebook Groups, at which time Defendant would have been removed from the Private Facebook Groups.

CLASS ACTION ALLEGATIONS

57. Plaintiff seeks to represent a class of all members of the Private Facebook Groups whose electronic communications were intercepted by Defendant (the "Class"). Plaintiff reserves the right to modify the class definition as appropriate based on further investigation and discovery obtained in the case.

58. Plaintiff also seeks to represent a subclass of all Class members in the State of Arizona who were members of the Private Facebook Groups, and whose electronic communications were intercepted by Defendant (the "Arizona Subclass"). Plaintiff reserves the right to modify the subclass definition as appropriate based on further investigation and discovery obtained in the case.

59. The Class and Arizona Subclass shall collectively be referred to as the "Classes."

60. Members of the Classes are so numerous that their individual joinder herein is impracticable. Specifically, there are over 33,000 members of the Private Facebook Groups. Members of the Classes may be notified of the pendency of this action by mail, publication through the distribution records of Defendant, and via Facebook.

61. Common questions of law and fact exist as to all members of the Classes and predominate over questions affecting only individual members of the Classes. Common legal and factual questions include, but are not limited to, whether Defendant has violated the Federal Wiretap Act, violated the Stored Communication

Act, and violated the common law right to privacy of Plaintiff and members of the Classes.

62. The claims of the named Plaintiff are typical of the claims of the Classes because the named Plaintiff, like all other class members, was a member of both Private Facebook Groups and had her electronic communications intercepted and/or accessed in electronic storage and disclosed to Defendant through the use of Defendant's wiretaps.

63. Plaintiff is an adequate representative of the Classes because her interests do not conflict with the interests of the members of the Classes she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of members of the Classes will be fairly and adequately protected by Plaintiff and her counsel.

64. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of members of the Classes. Each individual member of the Classes may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSES OF ACTION

COUNT I
Interception And Disclosure Of Electronic Communications In Violation Of The Federal Wiretap Act, 18 U.S.C. § 2511

65. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

66. Plaintiff brings this claim individually and on behalf of the members of the proposed Classes against Defendant.

67. As alleged herein, Defendant intentionally intercepted the electronic communications of Plaintiff and the proposed Classes.

68. Each of Defendant's wiretaps, automatic monitoring tools, processes, and software described herein, is an "electronic, mechanical, or other device" as defined by 18 U.S.C. § 2510(5) and is primarily used for the purpose of the surreptitious interception of electronic communications.

69. Upon information and belief, Defendant intercepts the electronic communications contemporaneously as they are sent.

70. Upon information and belief, Defendant receives and stores these messages through the employment of a mechanical or electrical tool or apparatus that is considered a device under 18 U.S.C §§ 2510, *et seq*.

71. Defendant's interception and internment of electronic communications sent between Plaintiff and members of the Classes is intentional, as alleged herein.

72. Plaintiff and members of the Classes did not consent to any of Defendant's actions in implementing wiretaps.

73. Defendant was not a party to any of these electronic communications.

74. Defendant's conduct violated 18 U.S.C. § 2511 and therefore gives rise to a claim under 18 U.S.C. § 2520.

75. Pursuant to 18 U.S.C. § 2520, Plaintiff and the Classes are entitled to the greater of actual damages or statutory damages or not less than $100 a day for each day of violation or $10,000, whichever is greater.

COUNT II

Manufacture, Distribution, Possession, And Advertising Of An Electronic Communication Interception Device In Violation Of The Federal Wiretap Act, 18 U.S.C. § 2512

76. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

77. Plaintiff brings this claim individually and on behalf of the members of the proposed Classes against Defendant.

78. 18 U.S.C. § 2512, in pertinent part, holds "any person" liable "who intentionally:"

> [M]anufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce.

18 U.S.C. § 2512(1)(b).

79. Each of Defendant's wiretaps, including the automatic monitoring tools and software described herein, are an "electronic, mechanical, or other device" as defined by 18 U.S.C. § 2510(5), and are primarily useful for the purpose of the surreptitious interception of electronic communications.

80. At all relevant times, by using automatic monitoring tools, software, and other processes and means employed by the STRATA team, Defendant intentionally manufactured, assembled, and/or possessed a device that is primarily useful for the purpose of surreptitious interception of electronic communications.

81. Defendant knew or had reason to know that its automatic monitoring tools, software, and other processes and means employed by the STRATA team—

which were transported through interstate commerce over the Internet—were primarily useful for the purpose of wiretapping electronic communications.

82. Plaintiff and members of the Classes did not consent to any of Defendant's actions in implementing wiretaps.

83. Defendant was not a party to any of these electronic communications.

84. Defendant's conduct violated 18 U.S.C. § 2512 and therefore gives rise to a claim under 18 U.S.C. § 2520.

85. Pursuant to 18 U.S.C. § 2520, Plaintiff and the Classes are entitled to the greater of actual damages or statutory damages or not less than $100 a day for each day of violation or $10,000, whichever is greater.

COUNT III
Violation Of The Stored Communications Act,
18 U.S.C. §§ 2701, *et seq*.

86. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

87. Plaintiff brings this claim individually and on behalf of the members of the proposed Classes against Defendant.

88. The Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701, *et seq*., prohibits "intentionally access[ing] without authorization a facility through which an electronic communication service is provided … and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701(a)(1).

89. The posts in the Private Facebook Groups are "electronic communications" delivered through an "electronic communications service" as defined in 18 U.S.C. § 2510(15).

90. At the time Plaintiff and the Classes' electronic communications were accessed without authorization on Facebook, the data was in "electronic storage" as required by the SCA. 18 U.S.C. § 2510(17).

91. At all relevant times, Defendant intentionally accessed the contents of Plaintiff's and members of the Classes' posts in the Private Facebook Groups, and thereby obtained the contents of posts in the Private Facebook Groups while the contents were in storage.

92. At all relevant times, Defendant acted without authorization.

93. Defendant was not a party to any of these electronic communications.

94. Plaintiff and members of the Classes are permitted to bring a civil action over these violations of the SCA. 18 U.S.C. § 2707(a).

95. Plaintiff and members of the Class seek all relief available under the SCA, including damages suffered by Plaintiff and members of the Classes for not less than $1,000, and punitive damages. 18 U.S.C. § 2707(c).

COUNT IV
Common Law Invasion Of Privacy/Intrusion

96. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

97. Plaintiff brings this claim individually and on behalf of the members of the proposed Classes against Defendant.

98. Plaintiff and members Classes have an interest in: (1) precluding the dissemination and/or misuse of their private posts in the Private Facebook Groups; and (2) being able to discuss local issues without observation, intrusion or interference, including, but not limited to, the right to join the Private Facebook Groups and interact with other Group Members without being subjected to wiretaps without Plaintiff's and members of the Classes' knowledge or consent.

99. As alleged above, Defendant intentionally intruded into conversations in which Plaintiff and members of the Classes had reasonable expectations of privacy. That intrusion occurred in a manner that was highly offensive to a reasonable person.

100. Defendant gained unwanted access to data by electronic and covert means, in violation of the law and social norms.

101. At all relevant times, through the wiretapping of the Private Facebook Groups, Defendant intentionally invaded Plaintiff's and members of the Classes' common law privacy rights.

102. Plaintiff and members of the Classes had a reasonable expectation that their posts in the Private Facebook Groups and would remain confidential and that Defendant would not infiltrate those groups and wiretap them. Indeed, such activity is expressly prohibited by Facebook's Terms of Use.

103. Plaintiff and members of the Classes did not consent to Defendant's wiretapping.

104. This invasion of privacy is serious in nature, scope and impact.

105. The invasion of privacy is sufficient to confer Article III standing.

106. This invasion of privacy alleged here constitutes an egregious breach of the social norms underlying the privacy right.

107. Plaintiff and members of the Classes seek all relief available for common law invasion of privacy claims under the law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order certifying the Classes under Rule 23 and naming Plaintiff as the representative of the Classes and Plaintiff's attorneys as Class Counsel to represent the Classes;

(b) For an order declaring that the Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

(d) For compensatory, punitive, and statutory damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief;

(g) For injunctive relief as pleaded or as the Court may deem proper; and

(h) For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit.

DEMAND FOR TRIAL BY JURY

Pursuant to Federal Rules of Civil Procedure 38(b), Plaintiff demands a trial by jury of all issues so triable.

Dated: June 21, 2022

Respectfully submitted,

WARD, KEENAN & BARRETT, P.C.

By: */s/ Gerald Barrett*
Gerald Barrett

Gerald Barrett, SBN: 005855
3838 N. Central Avenue, Suite 1720
Phoenix, Arizona 85012
Tel: (602) 279-1717
Fax: (602) 279-8908
E-Mail: gbarrett@wardkeenanbarrett.com

BURSOR & FISHER, P.A.
Neal J. Deckant (*Pro Hac Vice*)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ndeckant@bursor.com

BURSOR & FISHER, P.A.
Joshua D. Arisohn (*Pro Hac Vice*)
Alec M. Leslie (*Pro Hac Vice*)
Max S. Roberts (*Pro Hac Vice*)
888 Seventh Avenue
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jarisohn@bursor.com
aleslie@bursor.com
mroberts@bursor.com

Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on June 21, 2022, I electronically transmitted the foregoing to the Clerk's office using the CM/ECF System for filing and transmittal of a Notice of Electronic Filing to the following CM/ECF registrants:

David Michael Morrell
Jones Day - Washington, DC
51 Louisiana Ave. NW
Washington, DC 20001-2113
202-879-3939
Fax: 202-626-1700
Email: dmorrell@jonesday.com

John A Vogt
Jones Day - Irvine, CA
3161 Michelson Dr., Ste. 800
Irvine, CA 92612
949-851-3939
Fax: 949-553-7539
Email: javogt@jonesday.com

Ryan Ball
Jones Day - Irvine, CA
3161 Michelson Dr., Ste. 800
Irvine, CA 92612
949-553-7515
Email: rball@jonesday.com

Travis Monroe Wheeler
Bowman & Brooke LLP - Phoenix, AZ
2901 N Central Ave., Ste. 1600
Phoenix, AZ 85012
602-643-2310
Fax: 602-248-0947
Email: travis.wheeler@bowmanandbrooke.com

William Francis Auther
Bowman & Brooke LLP - Phoenix, AZ
2901 N Central Ave., Ste. 1600
Phoenix, AZ 85012
602-643-2409
Fax: 602-248-0947
Email: william.auther@bowmanandbrooke.com

s/Mary Farley